TWG-99-19

Federal PKI Directory Concept of Operations

19 February 1999

CYGNACOM SOLUTIONS

Suite 100 West♦7927 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF FIGURES

1 INTRODUCTION

The Federal Public Key Infrastructure (FPKI) is intended to support security services for communication between the public and government employees and between government employees associated with different agencies and organizations. A Federal Bridge Certificate Authority (BCA) has been proposed to cross-certify agency and organizational principal certificate authorities (PCAs), providing the necessary mapping information to support the verification of certificates between differing trust domains. However, the Federal BCA does not provide access to certificates, certificate revocation information, certificate policies, and certification practice statements for the trust domains. A separate Federal PKI Directory repository is required.

1.1 Purpose and Scope

This paper describes the architecture for a proposed Federal PKI Directory, composed of a collection of interconnected Border Directories. The paper addresses the interconnectivity of Border Directory System Agents (DSAs) with the Federal BCA DSA and agency-internal PKI infrastructures, provides a proposed concept of operation, examines protection issues, and describes a strategy for the evolution of the Federal PKI Directory.

1.2 Background

The Federal Public Key Infrastructure (PKI) will be constructed from numerous agency and organization PKIs. Some of these will be initially limited to particular applications (e.g., signature verification), but some will be agency-wide multi-application PKIs. Because of the nature of its composition, the Federal PKI cannot be a monolithic structure or a single enterprise PKI.

The approach adopted for the Federal PKI is based on the concept of a “bridge CA.” The bridge CA provides trust (or certification) paths between PCAs for the agency PKIs. Industry organizations and other nations are adopting similar solutions, where a designated CA cross-certifies with high level CAs in different trust domains, to create certification paths. This approach, illustrated in Figure 1, allows large-scale government, industry, national or global PKIs to be assembled from application or enterprise scale PKIs. The approach is further described in [TWG-98-29] and the Federal PKI Concept of Operations [CONOPS].

The Federal Bridge CA will provide cross-certification among the agency PKIs. Each agency PKI will designate a single principal CA to cross-certify with the Federal Bridge CA. The combination of a principal CA and its associated PKI form a domain of trust, wherein the principal CA provides a known point of trust for the domain. Agency PKIs currently use certification authority (CA) products and services from different vendors, and client products from many vendors.

To verify a digital signature, the relying party must build a certification path from the originator's certificate back to the certificate for an authority that the relying party trusts. For the bridge CA approach to work, Directory User Agents (DUAs) must be able to retrieve the certificates and certificate revocation information from trust domains cross-certified via the Federal Bridge CA. Border Directories, as described in this paper, provide the mechanisms to retrieve this information. The Bridge CA is cross-certified with the principal CA for the relying party's trust domain, enabling DUAs to build the necessary certification paths. Thus, the certification path can be built to the user's known point of trust.

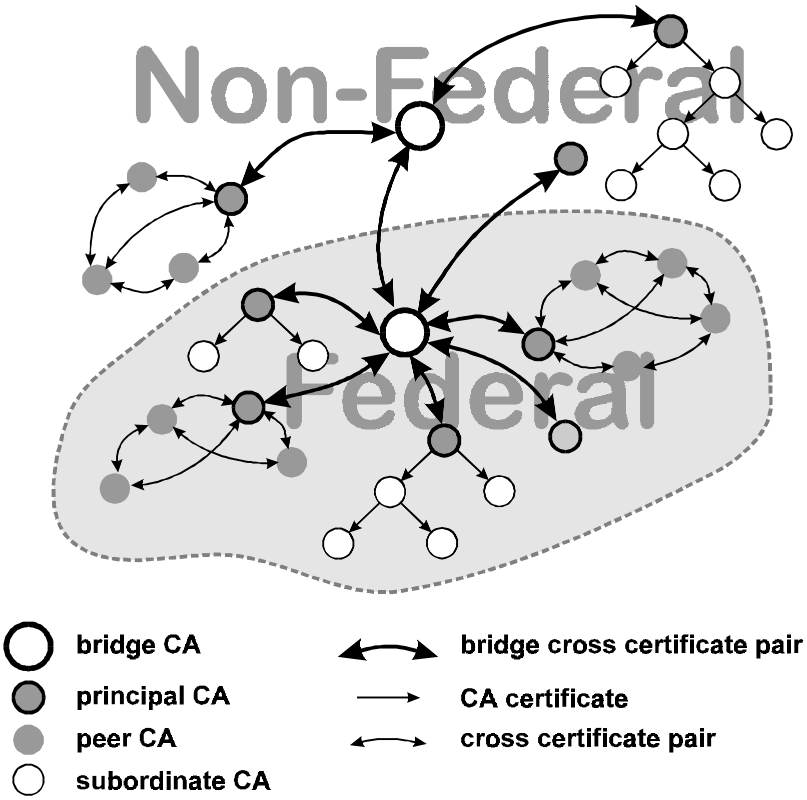

Figure 1. FPKI CERTIFICATION PATH ARCHITECTURE

2 BORDER DIRECTORY ARCHITECTURE

Border DSAs are intended to provide a mechanism for DUAs within Federal Government agencies to retrieve certificates and certificate revocation information from other agencies without the complexity of multiple directory access protocols. The Border DSAs will allow agencies to retain their existing directory infrastructures and still be able to communicate within the Federal PKI. The Border DSA would be a new, custom agency directory structure specifically created as part of the Federal PKI. Generally, each Border DSA would implement an “external” interface with the Bridge CA DSA and an “internal” interface to the Trust Domain that it serves.

2.1 Architectural Overview

Figure 2 illustrates the Bridge CA with its associated Directory System Agent (DSA). The Federal Bridge CA serves as a cross-certification entity for the Principal CA associated with each agency’s trust domain. Each agency PKI within the Federal PKI will be represented by a minimum of one Border DSA, which may be provided by the agency itself, outsourced to another agency, or outsourced to an external service provider.

Border DSAs will connect via the Bridge CA DSA to provide a government-wide certificate management repository. The Border DSA will provide each organization with an externally visible repository for certificates, certification revocation information, and certification practice statements. The Border DSA need not replicate the organization’s entire Directory Information Base (DIB).

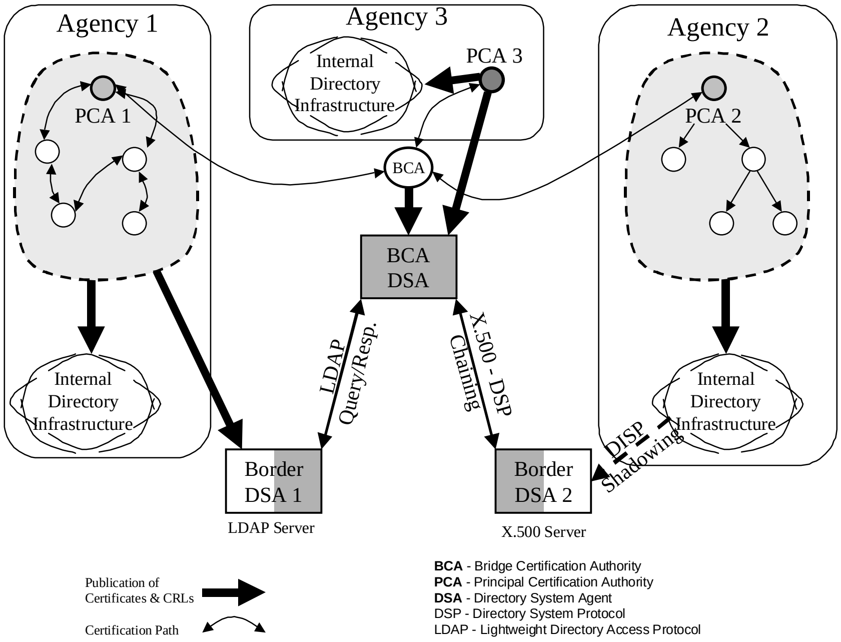
Agency 1
Agency 3
Agency 2
Internal Directory Infrastructure
PCA 3
PCA 1
PCA 2
BCA
BCA DSA
LDAP Query/Resp.
X.500 - DSP Chaining
Internal Directory Infrastructure
Internal Directory Infrastructure
DISP Shadowing
Border DSA 1
Border DSA 2
LDAP Server
X.500 Server
Publication of Certificates & CRLs
Certification Path
BCA - Bridge Certification Authority
PCA - Principal Certification Authority
DSA - Directory System Agent
DSP - Directory System Protocol
LDAP - Lightweight Directory Access Protocol

Figure 2. Federal Border Directory Architecture

Figure 2 illustrates the interconnection of three agencies, each having different internal directory structures, with the BCA DSA. (Note: external connections, such as the internet, are not included in the figure.) Agency 1 publishes certificate information to Border DSA 1 via an agency-internal protocol. The Border DSA is provided by the agency and supports the Lightweight Directory Access Protocol (LDAP) for queries and responses from other agency DSAs. Agency 2 publishes information from its internal directory to its Border DSA using the X.500 Directory Information Shadowing Protocol (DISP). The Border DSA supports the X.500 Directory System Protocol (DSP), using chaining to support queries and responses from other agency DSAs. Agency 3 does not have a separate DSA. Instead, the PCA is responsible for posting certificate information directly to the BCA DSA.

2.2 Federal Directory Components

The following are descriptions of entities involved with the Border Directory concept. The definitions and terms used are consistent with those defined in the Proposed Federal PKI Concept of Operation [Burr].

- *Trust Domains*: In the Federal context a trust domain is a portion of the Federal PKI that operates under the management of a single *policy management authority*. One or more Certification Authorities exist within the trust domain. Each trust domain has a single *principal CA*, but may have many other CAs. Each trust domain has a domain repository. In the non-Federal Context, trust domains, may be more loosely organized, but consist at a minimum of a group of CAs that share trust and operate under consistent policies. [Note: The internal trust domain of an agency is, for the purpose of this paper, separate and distinct from that agency's trust domain as a portion of the Federal PKI. Certificate information relative to the internal domain of an agency may not be completely available via the Federal PKI.]

- *Federal Policy Management Authority (FPMA)*: this management authority sets the overall policies of the Federal PKI, and approves the policies and procedures of trust domains ***within*** the Federal PKI. It operates a Federal Bridge CA, and repository. [Note: The FPMA is the management authority for agencies' "external" trust domains.]

- *Domain Policy Management Authorities (DPMA)*: a policy management authority approves the certification practice statements of the CAs within a trust domain, and monitors their operation. The DPMAs operate or supervise a domain repository. In the non-federal context, a DPMA may be an association of CAs that share trust and use consistent or comparable CA policies. [Note: The DPMA is the management authority for an agency's internal trust domain.]

- *Certification Authorities (CA)*:
    - ◊ *Bridge CA (BCA)*: the Federal Policy Management Authority operates the Federal Bridge CA. Its purpose is to be a bridge of trust that provide trust paths between the various trust domains of the Federal PKI, as well as between the Federal PKI and non-federal trust domains. FPMA approved trust domains designate a principal CA that is eligible to cross-certify with the Federal BCA. Note that the BCA is not a *root CA*, since it does not ordinarily begin certification paths. When the BCA cross certifies with CAs it may include nameConstraints, pathLengthConstraints or policyConstraints that limit the propagation of trust to other, cross-certified domains. The BCA also issues a consolidated Federal ARL.
    - ◊ *Principal CA*: A CA within an (external) trust domain that cross-certifies with the Federal BCA. Each trust domain has one principal CA. In the case of a domain with hierarchical certification paths, it will be the root CA of the domain. In a mesh-organized domain, the principal CA may be any CA in the domain. However it will normally be one operated by, or associated with, the domain policy management authority.

- *Repositories (Border DSAs)*: Repositories are on-line facilities that provide certificates and certificate status information. Repositories in the Federal PKI will provide information via the LDAP protocol or X.500 DSP chained operations, but they may also provide information in other ways. The FPMA will maintain an open repository for CA certificates and revocations. Repositories that contain end-entity certificates and CRLs for end-entity certificates, or other certificate status responders, are referred to as "Border DSAs."

- *BCA Repository (BCA DSA)*: The BCA repository will be open to Internet access by anyone, and will make the following available:
  - All certificates issued by the BCA;
  - All certificates held by the BCA;
  - All cross certificate pairs containing certificates held or issued by the BCA;
  - All CA certificates issued by CAs within the overall Federal PKI;
  - All cross certificate pairs between CAs in the Federal PKI;
  - A consolidated Federal ARL that covers all CAs in the Federal PKI. This implies a requirement to include appropriate CRL Issuer and CRL Distribution Point extensions in all CA Certificates issued by CAs within the Federal PKI;
  - Other certificates and CRLs as determined by the FPMA;

2.3 Concept of Operation

Border DSAs must address both incoming directory requests (i.e., originating outside the agency's trust domain) and outgoing directory requests (i.e., originating within the agency's trust domain).

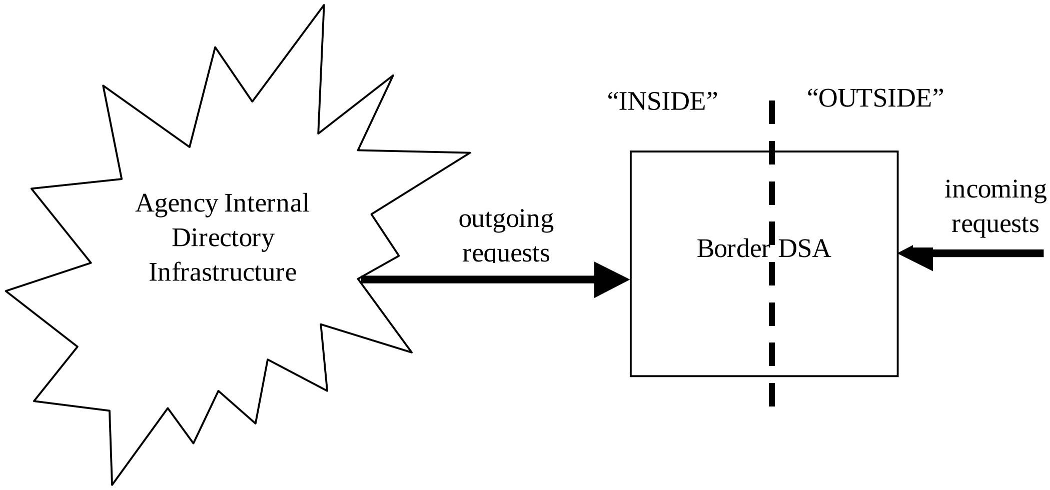

Figure 3. Directory Information Flows

2.3.1 Incoming Requests

A basic assumption is that incoming directory requests will always arrive from (or via) either the BCA DSA or another Border DSA. Thus, the Border DSA's external interface (i.e., the interface provided to the "outside" from an agency) may limit requests to only those received from other Border DSAs or the BCA DSA. Such "external" directory communications among the Border DSAs and the BCA DSA will be limited to X.500 DSP chained operations or LDAP queries and responses. One or more separate "public" Border DSAs may be provided to support public access to the FPKI. The alternative of providing *direct* public access to an organization's internal directory infrastructure or to an organization's Border DSA is unacceptable.

2.3.2 Outgoing Requests

In general, outgoing requests (originating inside the agency's trust domain) can be presented to the internal interface of the agency's Border DSA using any protocol specified by the agency. If the protocol is not one of those supported on the external side of the Border DSA, the Border DSA must reformat outgoing requests and present them to the destination Border DSA using either of the supported protocols. In this manner, the Border DSAs will be capable of obtaining information (including certificates, CRLs, or CPSs) from external Border DSAs on behalf of DUAs within their trust domains.

3 PROTECTION ISSUES

A significant area of concern is how to protect the organization's internal directory infrastructure from attacks through the Border DSA. Although it may seem to be cross-purposes, the FPKI directory infrastructure is intended to provide public access to Federal PKI certificate information while at the same time preventing any serious threat against attacks against the infrastructure.

In this section, the issue of protecting both the FPKI directory and the agencies' internal infrastructures is examined from two perspectives: (1) limiting disclosure and (2) limiting malicious input.

3.1 Limiting Disclosure from the Internal Directory Infrastructure

The only communications between an agency's internal directory infrastructure and its Border DSA should be for the purposes of posting appropriate new information from the internal infrastructure out to the Border DSA and in support of certificate verification by agency-internal relying parties. The guidance for what to post could be stated as, "Post anything you wouldn't mind seeing on the front page of the New York Times." By identifying who is authorized to post information and exactly what type of information may be posted, an agency can gain some control over both disclosure and malicious modification from within the trusted domain. The following approaches (in decreasing order of strength) can be used to control posting:

- Separate administrative posting ("air gap"): The Border DSA performs an authentication check against the administrator, who must be authorized to post the information. The administrator without a network connection posts the information between the internal infrastructure and the Border DSA (e.g., via a diskette or other mountable media). Administrator posting to the Border DSA should be audited and the audit logs periodically inspected.

- Administrative posting from domain infrastructure: The Border DSA performs an authentication check against the administrator, who must be authorized to post the information. The administrator posts the information over a network connection between the internal infrastructure and the Border DSA. Administrative posting to the Border DSA should be audited and the audit logs periodically inspected.

.

- Replication (shadowing) from domain infrastructure: A DSA inside the agency's internal directory infrastructure is designated as a "Master" DSA with a shadowing agreement to the Border DSA that identifies specific directory subtrees to replicate to the Border DSA. The shadowing agreement should specify supplier-initiated shadowing.

- User posting from domain infrastructure: Any user inside the agency's internal infrastructure can post anything to the Border DSA. This approach is not recommended, but is included for completeness. In the event that this approach is deemed adequate by an agency, user posting to the Border DSA should be carefully audited and the audit logs periodically inspected.

3.2 Limiting Malicious Input to the Internal Directory Infrastructure

The only external information flows from a Border DSA should be to provide a relying party with information legitimately posted to the Border DSA or to forward a legitimate request to another Border DSA or the BCA DSA. In particular, an agency should not use its Border DSA to chain into its own internal directory infrastructure (e.g., by using knowledge references). Outside access to the internal directory infrastructure should use an entirely separate access path from the Federal PKI. The separate path should be suitably protected (e.g., network-level firewalls and proxies, application-level active firewalls, encrypted dial-up access, or guards) or suitable cryptographic protections (e.g., message authentication codes, digital signatures, or encryption) should be applied to the transmitted or received information.

3.3 Limiting Malicious Input to the Border Directory

External users (i.e., users from other agencies or the public) should not be able to post anything to the Border DSA. In the event that an agency wants to post external user information, it is recommended that (1) the information be submitted to an administrator using an out-of-band mechanism (e.g., digitally signed email or secure web transaction), (2) the administrator use suitable means to ensure the "goodness" of the information, and (3) that the administrator post the information using one of the foregoing mechanisms.

4 FEDERAL PKI DIRECTORY EVOLUTION

The Federal PKI Directory will be an evolutionary enterprise. The initial Federal Directory will include X.500 Border DSAs and BCA DSA that intercommunicate using only DSP chained operations. The second capability would extend the BCA DSA to provide support for LDAP servers. Whether the initial LDAP fielding will provide interoperability between LDAP Border DSAs and X.500 Border DSAs is still a question.

The goal is to provide a Border DSA to host each agency's externally-accessible certificate information. This does not, however, mean that each agency is expected to "stand up" its own Border DSA. Some agencies have indicated a willingness to host the certificate information for "subscriber" agencies on their system. Such subscriber agreements could help in populating the Federal PKI Directory in the near term. A more long-term approach is for agencies to engage an external contractor to provide the Border DSA service on their behalf.

Finally, the U. S. Government On Line Directory (USGOLD) is already positioning itself as the Federal Government's directory for telephone and email access. It is unclear whether the BCA and Border DSAs and the USGOLD will eventually coalesce and, if so, how they will be combined.

5 SUMMARY

The following are features of the Border Directory concept:

- Does not require DUAs to handle different directory access protocols (LDAP v2, LDAP v3, DAP, etc.)
- Requires that participating Trust Domains populate a subset of PKI information on at least one Border DSA
- Requires that at least one agency develop and host a Border DSA
- Does not require changes to legacy applications
- Does not impact CA to Directory/Repository protocols or interactions
- Allows agencies to implement local policies regarding who accesses which directory entries

In addition, the directory needs to provide the Certificate Policies (CP) and Certification Practice Statements (CPS) [CHOK] to users of the Federal PKI.

REFERENCES

[BURR] Proposed Federal Public Key Infrastructure Concept of Operations, 4 September, 1998

[CHOK] Certificate Policy and Certification Practices Framework, S. Chokhani and W. Ford, Informational RFC, IETF PKIX Part IV, July 1997.

[CONOPS] TWG-98-31, *Draft Federal PKI Concept of Operations*, 3 June 1998

[TWG-98-29] W. E. Burr, “Proposed Federal PKI Architecture,” 19 May 1998